AMENDMENT TO THE SPECIFICATION

Please replace paragraph 0004 with the following amended paragraph:

[0004] The deployment, configuration and management of enterprise networks often requires specially-trained personnel tasked with installing and maintaining the network devices implementing or supporting the networks. For example, after physical installation of the network device, a network administrator typically must access a configuration interface to provide initial configuration information, such as an IP address and subnet mask. Accordingly, the cost and ability to manage and maintain enterprise networks can become problematic, especially for enterprises with a number of remote facilities. For example, the deployment and configuration of a given network device often requires an enterprise, or network service provider, to send out skilled personnel to perform the required installation and configuration tasks. In large enterprise networks, the ability to, as well as the costs associated with, deploying a large number of network devices can become problematic. While some network devices include functionality (such as Layer 2 discovery mechanisms) allowing them to be automatically configured by a network management device after physical installation on a network, these automated deployment mechanisms are typically limited to local installations where the configuring system and the newly-deployed network device are on the same subnetwork. Given the vast array of enterprise network topologies discussed above, methods, apparatuses and systems are required to facilitate automated, remote deployment of network devices. Embodiments of the present invention substantially fulfill this need. The deployment, configuration and management of enterprise

networks further requires network security, which may entail encryption of key network configuration parameters or messages. As known by those of skill in the art, there are two primary types of encryption algorithms, known as "symmetric encryption" or "asymmetric encryption" algorithms. Symmetric cryptography, also known as "secret key cryptography," is a system in which a single secret key is used to encrypt or decrypt a message. It is symmetric in the sense that both sender and receiver have the same key, and senders can decrypt any message sent to the receiver using the secret key. Asymmetric cryptography is also known in the art as "public-key cryptography." A common public-key system is known as the "RSA public key cryptosystem." See Thomas H. Cormen, Charles E. Leiserson, Robert L. Rivest, and Clifford Stein, ***Introduction to Algorithms, Second Edition***, MIT Press and McGraw-Hill, 2001, ISBN 0-262-03293-7, *Section 31.7: The RSA public-key cryptosystem*, pp. 80-81. In a public-key cryptography system, a user has two keys, a private key and a public key. The private key is kept secret, while the public key may be widely distributed to various potential senders. The private key cannot by determined in a practical manner from the public key, and a message encrypted with the public key can be decrypted only with the private key. Thus, access to keys and messages is asymmetric, in that the senders have a different key from the receiver, and only the receiver can decrypt the various sent messages. This ensures the various users of confidentiality. Various asymmetric encryption algorithms are described in Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone, ***Handbook of Applied Cryptography***, CRC Press, October 1996, ISBN 0-8493-8523-7, and R. Rivest, A. Shamir, and L. Adleman, ***Method for Obtaining Digital Signatures and Public –Key Cryptosystems***, Communications of the ACM, Vol. 21 (2),

pp. 120-126, 1978.

Please replace paragraph 0018 with the following amended paragraph:

[0018] When a given network device 30 responds to the initial configuration message, in one implementation, configuration interface module 150 of network device 30 establishes a connection by transmitting a configuration request (e.g., an LDAP request, an HTTP request, etc.) to network management system 43. In one implementation, the configuration request includes the network device name and password provided in the initial configuration message. In one implementation, this information is encrypted using ~~the same~~ encryption keys, as discussed below ~~above~~. In one implementation, when network management system 43 receives a configuration request, it retrieves the encryption key corresponding to the source IP address in the configuration request and decrypts the configuration request (222). Using either the source IP address or the network device identifier in the configuration request, network management system 43 then determines whether the network device 30 is on the pending list (224). If so, network management system 43, in one implementation, removes network device 30 from the pending list and adds it to a configured list (226). In one implementation, network management system 43 can perform other actions as well, such as, notifying a network administrator (228). Otherwise, network management system 43 initiates a standard configuration work flow (230)—that is, the configuration request, in one implementation, is handled similarly to configuration requests from previously configured network devices. For example, network device 30 both in this instance and in subsequent configuration sessions pulls its configuration information from network management system 43, writing the retrieved configuration information into its files and memory structures as appropriate.

Please replace paragraph 0028 with the following amended paragraph:

[0028] In other implementations, alternative encryption key components can be used. For example, the secret string can be unique to different types, classes, or groups of network devices. In one implementation, the secret string can be a random string stored on network device 30 during the manufacturing process. In another implementation, additional key components can include the network device serial number of MAC address associated with a network interface. In other implementations, the encryption key may further include a time stamp, as with the random number the time stamp value can also be included in plain text in the RSVP PATH message. Still further, alternative encryption schemes involving asymmetric (or public key) encryption algorithms can be used, where the configuration information (or the symmetric encryption keys) are encrypted using a private key associated with network management system 43. In such an implementation, the network device 30 is configured with ~~the~~ a public key and is able to decrypt the configuration information (or the encryption keys).